Admins - Anomalie #1655

Spam via le formulaire de contact à stopper

30/04/2015 18:22 - Frédéric Couchet

Statut:	Fermé	**Début:**	30/04/2015
Priorité:	Normale	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	90%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

nous recevons du Spam depuis quelques jours via notre formulaire de contact <http://www.april.org/contact>. Pour chaque catégorie de demande de contact, il y a des destinataires spécifiques.

Comme c'est le Drupal qui gère l'envoi des courriels, pas sûr que blacklister les adresses d'expéditeur suffisent, je ne sais pas.

Ci-dessous un exemple de courriel (j'ai malheureusement effacé les autres) :

From mad Mon Apr 27 10:43:02 2015
Return-Path: <www-data@april.org>
Received: from smtp.drieu.org [176.31.119.197]
by absinthe.couchet.org with POP3 (fetchmail-6.3.26)
for <mad@localhost> (single-drop); Mon, 27 Apr 2015 10:43:02 +0200 (CEST)
Received: from taverne.drieu.org (localhost.localdomain [127.0.0.1])
by taverne.drieu.org (Cyrus v2.4.16-Debian-2.4.16-4+deb7u2) with LMTPA;
Mon, 27 Apr 2015 10:07:51 +0200
X-Sieve: CMU Sieve 2.4
Received: by taverne.drieu.org (Postfix, from userid 8)
id E0182E1C23; Mon, 27 Apr 2015 10:07:51 +0200 (CEST)
X-Spam-Checker-Version: SpamAssassin 3.3.2 (2011-06-06) on taverne.drieu.org
X-Spam-Level:
X-Spam-Status: No, score=-1.0 required=5.0 tests=BAYES_00,FORGED_HOTMAIL_RCVD2,
FREEMAIL_FROM,T_TO_NO_BRKTS_FREEMAIL,WEIRD_PORT autolearn=no version=3.3.2
Received: from storm.april.org (storm.april.org [62.210.247.186])
by taverne.drieu.org (Postfix) with ESMTPS id 9CFBBE1BA6
for <frederic@couchet.org>; Mon, 27 Apr 2015 10:07:47 +0200 (CEST)
Received: by storm.april.org (Postfix)
id A82754BD06D; Mon, 27 Apr 2015 10:04:12 +0200 (CEST)
Delivered-To: fcouchet@april.org
Received: from localhost (unknown [192.168.2.16])
by storm.april.org (Postfix) with ESMTP id 4CB3D4BD06B;
Mon, 27 Apr 2015 10:04:12 +0200 (CEST)
Received: from storm.april.org ([192.168.2.17])
by localhost (spamvir.april.org [192.168.2.16]) (amavisd-new, port 10024)
with ESMTP id fBjPvewFAoTs; Mon, 27 Apr 2015 10:04:10 +0200 (CEST)
Received: from relay.april-int (ns1.april.org [88.191.250.4])
(using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
(No client certificate requested)
by storm.april.org (Postfix) with ESMTPS id EB3CE4BD04A;
Mon, 27 Apr 2015 10:04:09 +0200 (CEST)
Received: from ns1.april.org (lsd.april-int [192.168.1.42])
by relay.april-int (Postfix) with ESMTP id DD74D2A49E8;
Mon, 27 Apr 2015 10:04:09 +0200 (CEST)
Received: by ns1.april.org (Postfix, from userid 33)
id D182A17A12F; Mon, 27 Apr 2015 10:04:09 +0200 (CEST)
To: fcouchet@april.org,jtadeusz@april.org,contact@april.org
Subject: =?UTF-8?B?W0Rvc3NpZXJzIChEUk0sIGJyZXZldHMsIHZlbnRlIGZvcmPDqWUsIMOpZHVjYXQ=?=
=?UTF-8?B?aW9uLCBlbnRyZXByaXNlcy4uLildIHV3cGl3YyBuZWNrbGluZS4gIFdoZW4gaXQ=?=
=?UTF-8?B?IGNvbWVzIHRvIGEgc3RyYXBsZXNzIG5lY2tsaW5lLCB0aGVyZSBpcyBhIHdpZGU=?=

=?UTF-8?B?ciBjaG9pY2Ugb2Ygd2VhcmluZyBjb3N0dW1lIGpld2VscnkuICBXZWFyaW5nIGE=?=
=?UTF-8?B?IHBlYXJsIG5lY2tsYWNlLCB3aGV0aGVyIGl0J3MgdGhlIHJlYWwgdGhpbmcgb3I=?=
=?UTF-8?B?IGEgY29zdHVtZSAgcXV1ZWJrIG1yc2V4aSBtZnk=?=
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8; format=flowed; delsp=yes
Content-Transfer-Encoding: 8Bit
X-Mailer: Drupal
Errors-To: contact@april.org
Sender: contact@april.org
From: sapidqdna@hotmail.com
Message-Id: <20150427080409.D182A17A12F@ns1.april.org>
Date: Mon, 27 Apr 2015 10:04:09 +0200 (CEST)
X-Bogosity: Unsure, tests=bogofilter, spamicity=0.500000, version=1.2.4
Content-Length: 1611
Lines: 25

Curtisgdwud a envoyé un message via le formulaire de contact sur
https://www.april.org/contact.

for casual to elegant dress, and is a wonderful way to express your
personality. Also you want to learn how to analyze the jewelry store
competition, this way you will be <a
href="http://www.industrialsystech.com/pages/fany/">engagement rings yellow
gold you can simply hunt for them on the online jewelry store that you
have selected. The best time to do this is after a major holiday as most of
the charm it and emerald-cut
moonstone ringsâ€”skew romantic with an undercurrent of edge. Thistle
and Clover is just as much a clothing store as it is a jewelry destination,
but the Fort Greene boutique's <a
href="http://www.samer.no/wp-content/fany/">tiffany scissor necklace
jewelry trademark is the marking on the piece of jewelry which dictates who
in fact manufactured the piece of jewelry. It is a way for the artisan or
jewelry manufacturer <a
href="http://blog.generace.co.jp/wp-content/fany/">how to know your ring
size dentistry, medical equipment, fuel cells) as well as in the
manufacturing of beautiful pieces of fine jewelry. While working in various
capacities in the jewelry industry,Â Samantha began to notice the number <a
href="http://gys.strong-mart.com:8000/pages/fany/index.asp">sizing your ring
finger you will get what you must be looking for. Mike Cena is a jewelry
designer at ibraggiotti and specialist in ichthus wedding rings and fine
bridal jewelry visit our online Fine

Historique

#1 - 30/04/2015 18:25 - Frédéric Couchet

sur la VM nginx de ns1 :

grep "GET /contact" /var/log/nginx/www.april.org/www.april.org.access_log donne notamment

91.200.12.72 - - [30/Apr/2015:16:56:29 +0200] "GET /contact HTTP/1.0" 200 17416 "http://www.april.org/contact" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.124 YaBrowser/14.10.2062.12521 Safari/537.36"

91.200.12.66 - - [30/Apr/2015:10:43:09 +0200] "GET /contact HTTP/1.0" 200 17416 "http://www.april.org/contact" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.71 Safari/537.36"

Visiblement les spams sur le formulaire de contact viennent d'adresses en 91.200.12.XX

#2 - 30/04/2015 18:28 - Frédéric Couchet

On blackliste le réseau d'adresses :

sur la VM nginx de ns1, modification de /etc/nginx/sites-enabled/01_www.april.org pour ajouter la ligne :

```
deny 91.200.12.0/24;
```

redémarrage du service nginx

Dans les logs ensuite :

91.200.12.72 - - [30/Apr/2015:18:18:18 +0200] "GET /contact HTTP/1.0" 403 564 "http://www.april.org/contact" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.124 YaBrowser/14.10.2062.12061 Safari/537.36"

Le 403 (access denied) apparait bien

#3 - 30/04/2015 18:38 - Frédéric Couchet

- Statut changé de Nouveau à En cours de traitement

- % réalisé changé de 0 à 90

#4 - 14/02/2016 11:37 - François Poulain

- Statut changé de En cours de traitement à Fermé

#5 - 25/12/2020 23:49 - Christian P. Momon

- Description mis à jour

- Assigné à mis à François Poulain